

SecureNet

**Department of Energy
Defense Program
Wide Area Network**

Peter Dean

Sandia Release # 97-8607c

SecureNet's Mission

Support:

- | Accelerated Strategic Computing Initiative (ASCI)**
- | Advanced Design and Production Technologies Initiative (ADAPT)**

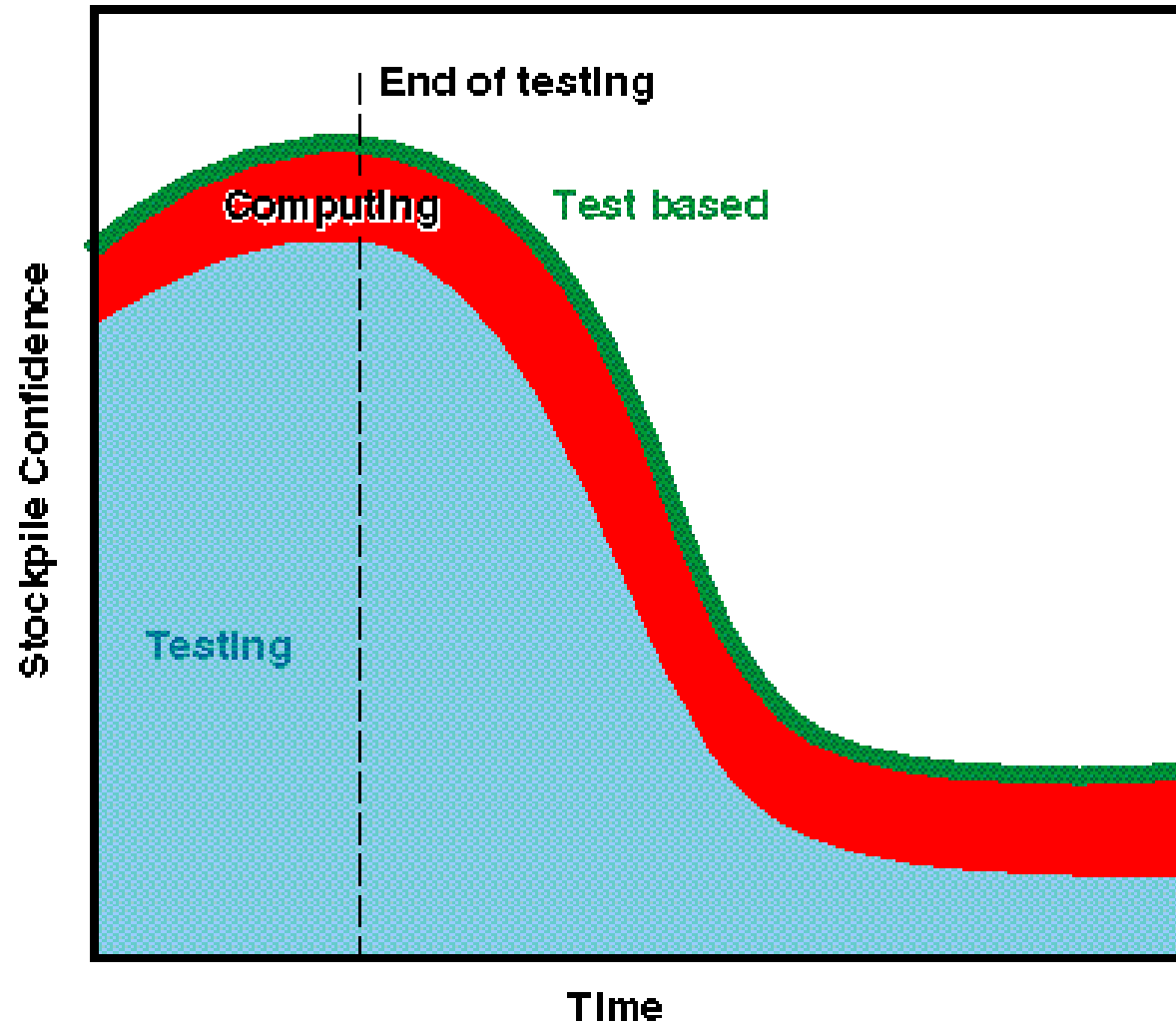
ASCI's vision is to:

Create leading-edge computational modeling and simulation capabilities critically needed to

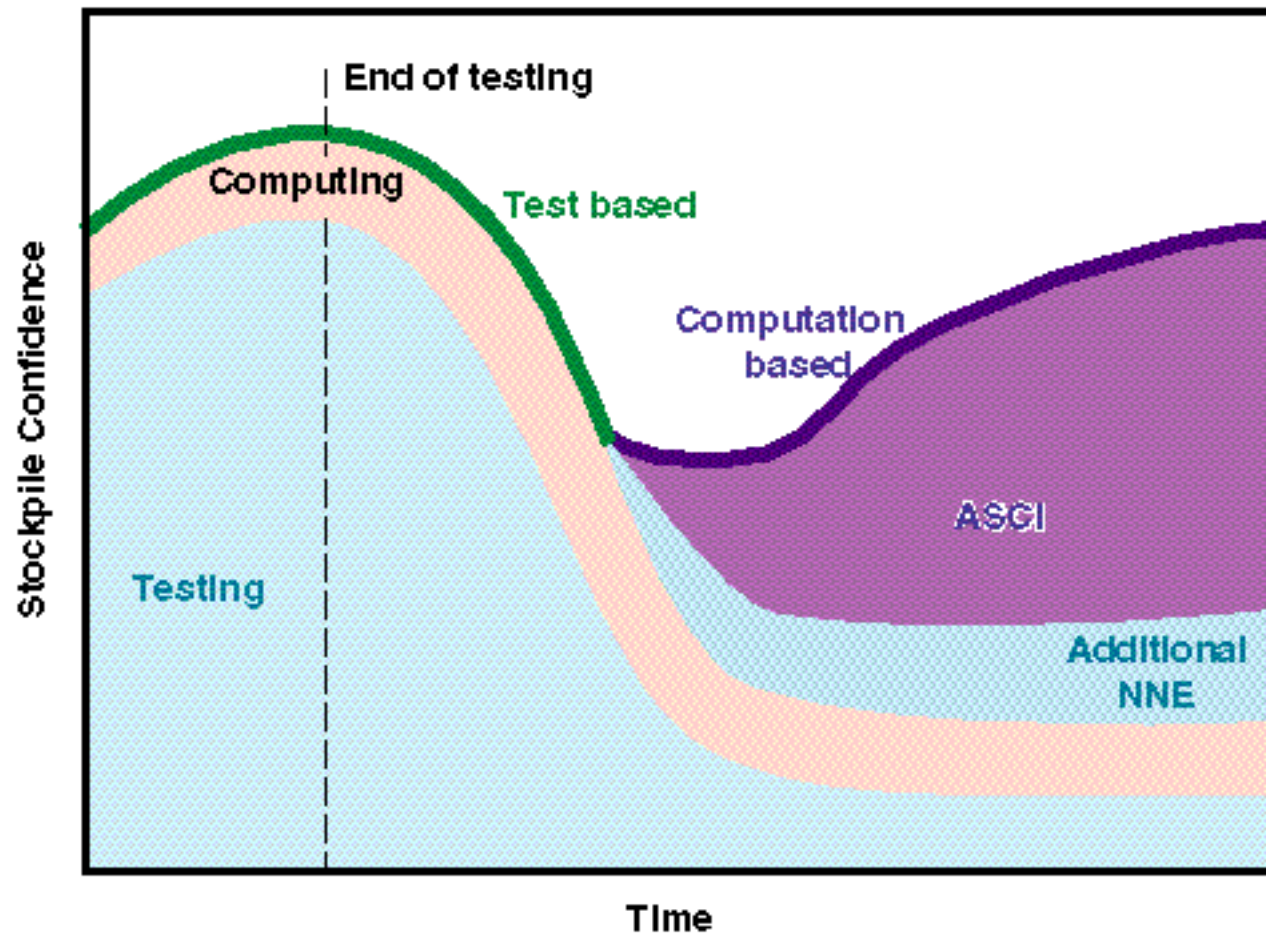
**promptly shift from
nuclear test-based methods
to *computational-based methods*,**

**to integrate stockpile stewardship elements
and thus reduce the nuclear danger**

Today's computing and simulation capabilities are nuclear-based design tools, not performance predictors

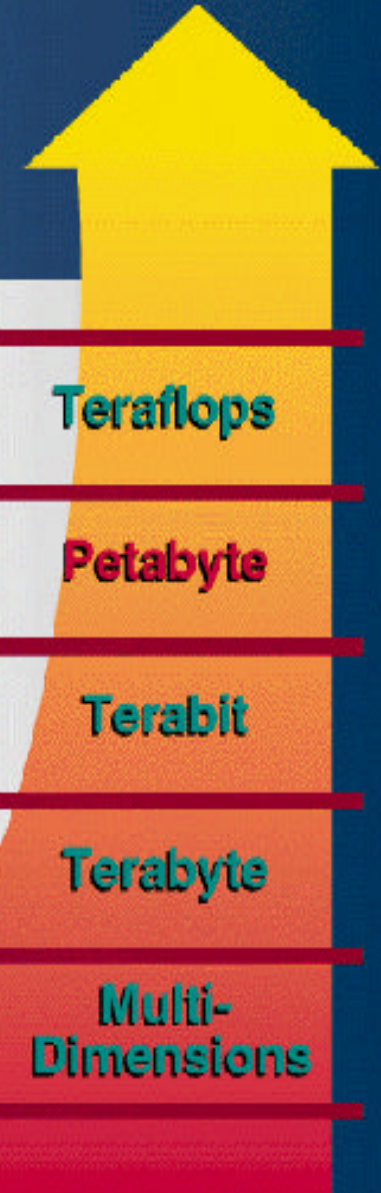


ASCI will make the paradigm shift in stockpile confidence



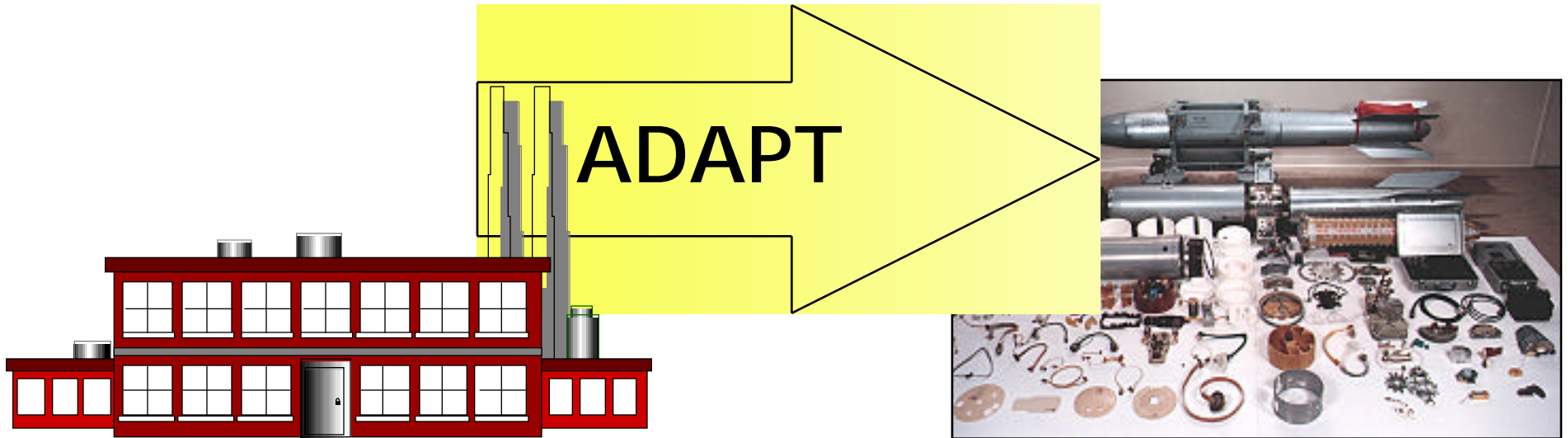
Capacity and Performance

Balance or Bottleneck



Processors	Kiloflops	Megaflops	Gigaflops	Teraflops
Archive	Megabyte	Gigabyte	Terabyte	Petabyte
Network /sec	Kilobit	Megabit	Gigabit	Terabit
Memory Size	Kilobyte	Megabyte	Gigabyte	Terabyte
Calculations	1-D	2-D	3-D	Multi-Dimensions
	1970's	1980's	1990's	Year 2000

Advanced Design & Production Technologies Initiative



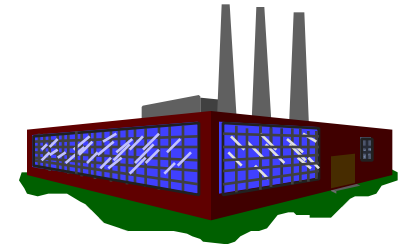
A Program to modernize, revitalize and transform the Nuclear Weapons Production Complex for the 21st Century.

ADAPT GOALS

Reduce Defects and Cycle Time . . . Lower Cost

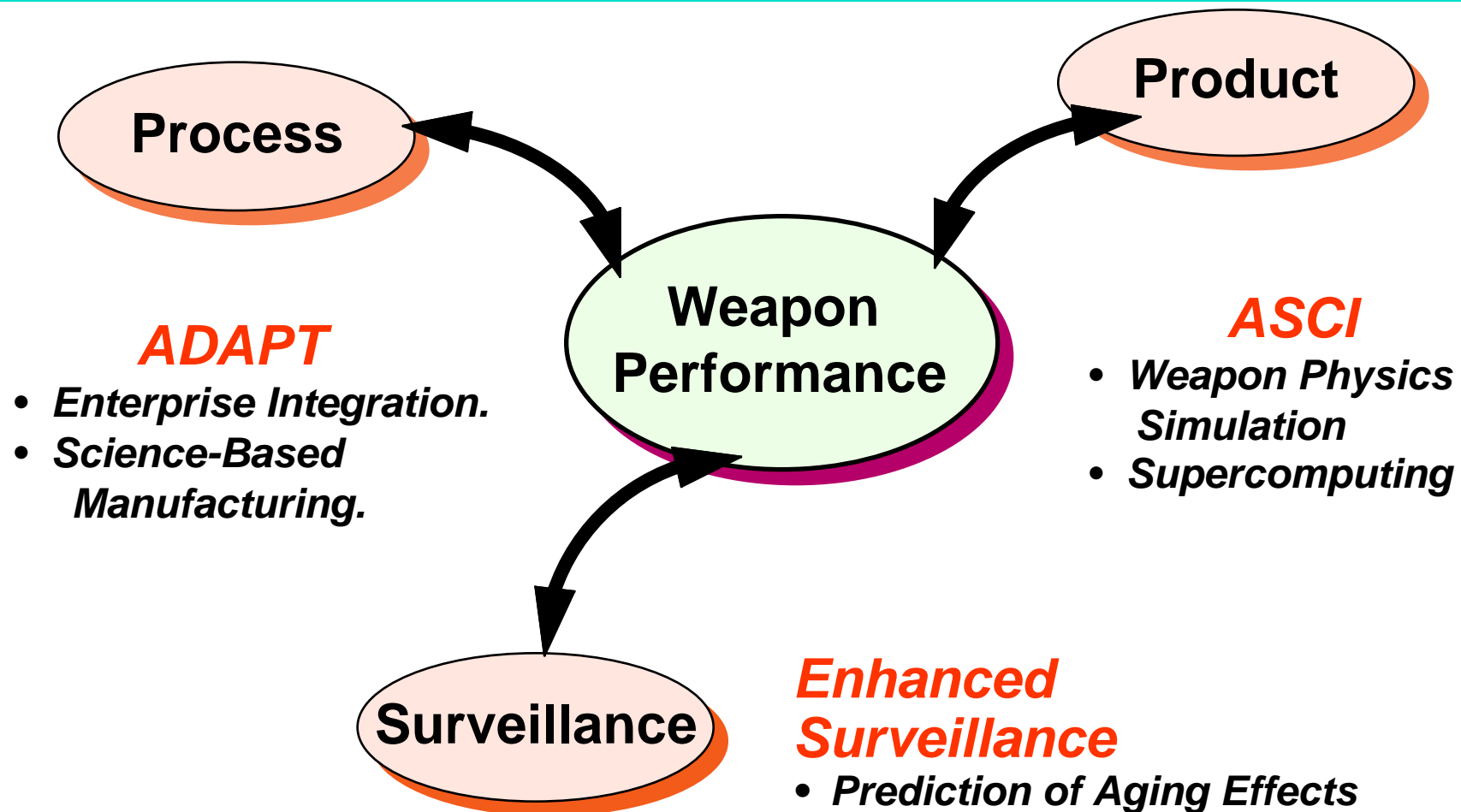
- Reduce Defects by 1- order of magnitude (1 to 0.1 per year).
- Cut time to respond by One Half (3 - 4 years to 18 months).

American Industry is doing it !



- Boeing . . . 30% cost savings; 67% inspection reduction.
- McDonnell Douglas . . . 68% fewer drawings; 58% scrap reduction.
- Hewlett Packard . . . 35% less development time; 60% lower field failures.
- John Deere . . . 30% development cost savings; 60% time reduction.
- Ford, Chrysler . . . significant reduction in defects and inspection time.

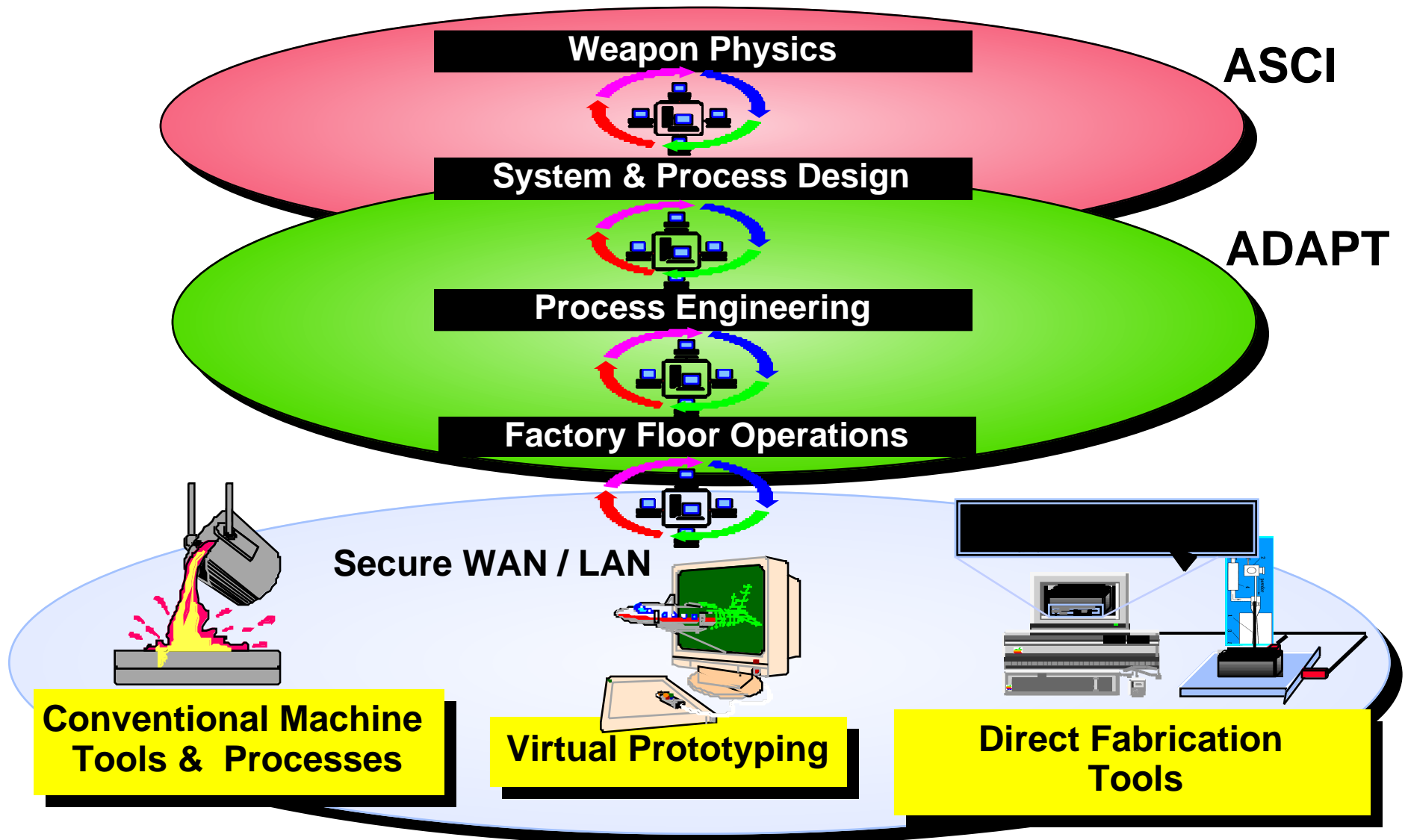
DP Strategy Draws on Three New Initiatives



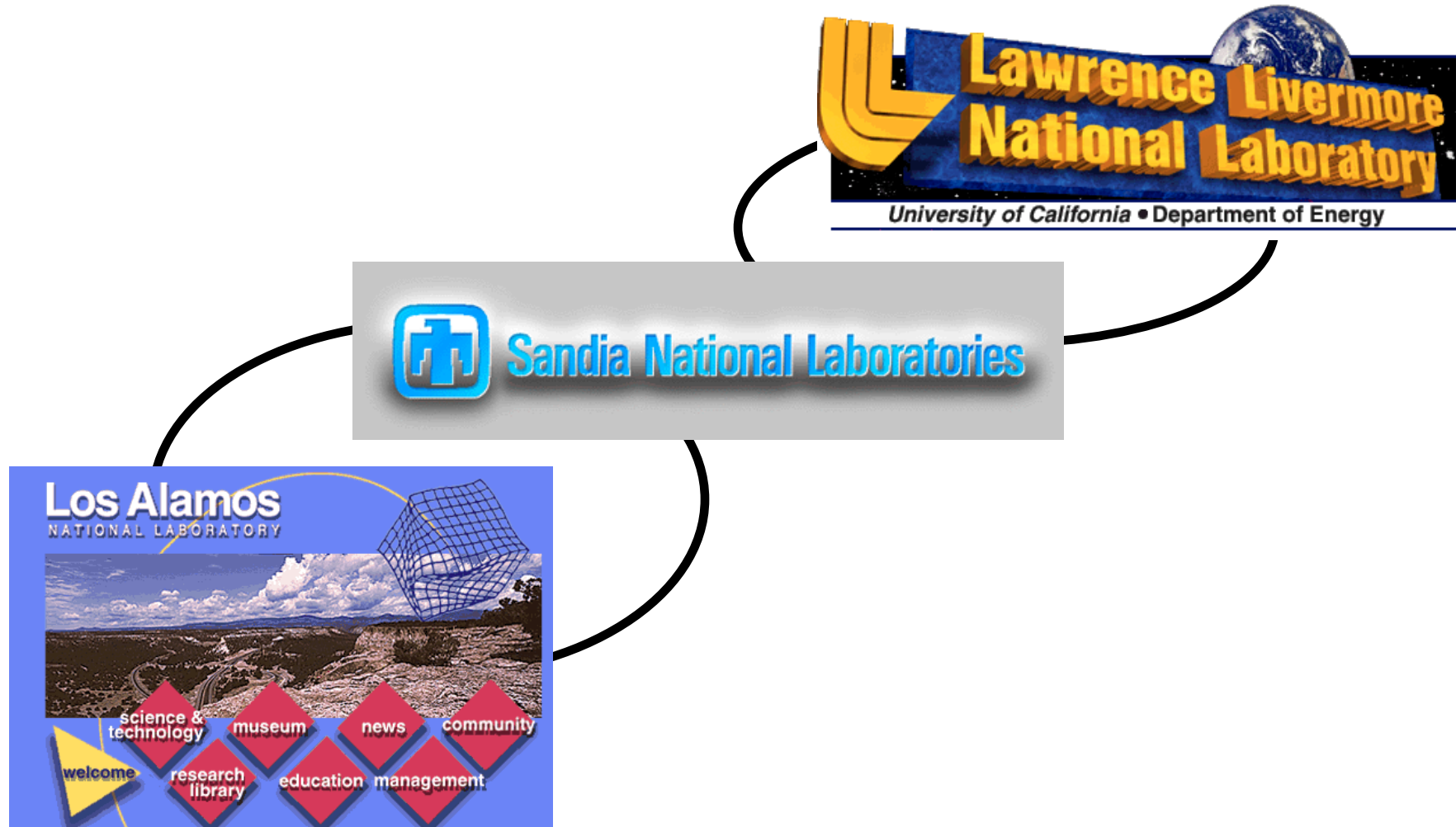
Assuring Performance through Modeling and Simulation

ADAPT Vision is Simulation - Based Product Realization

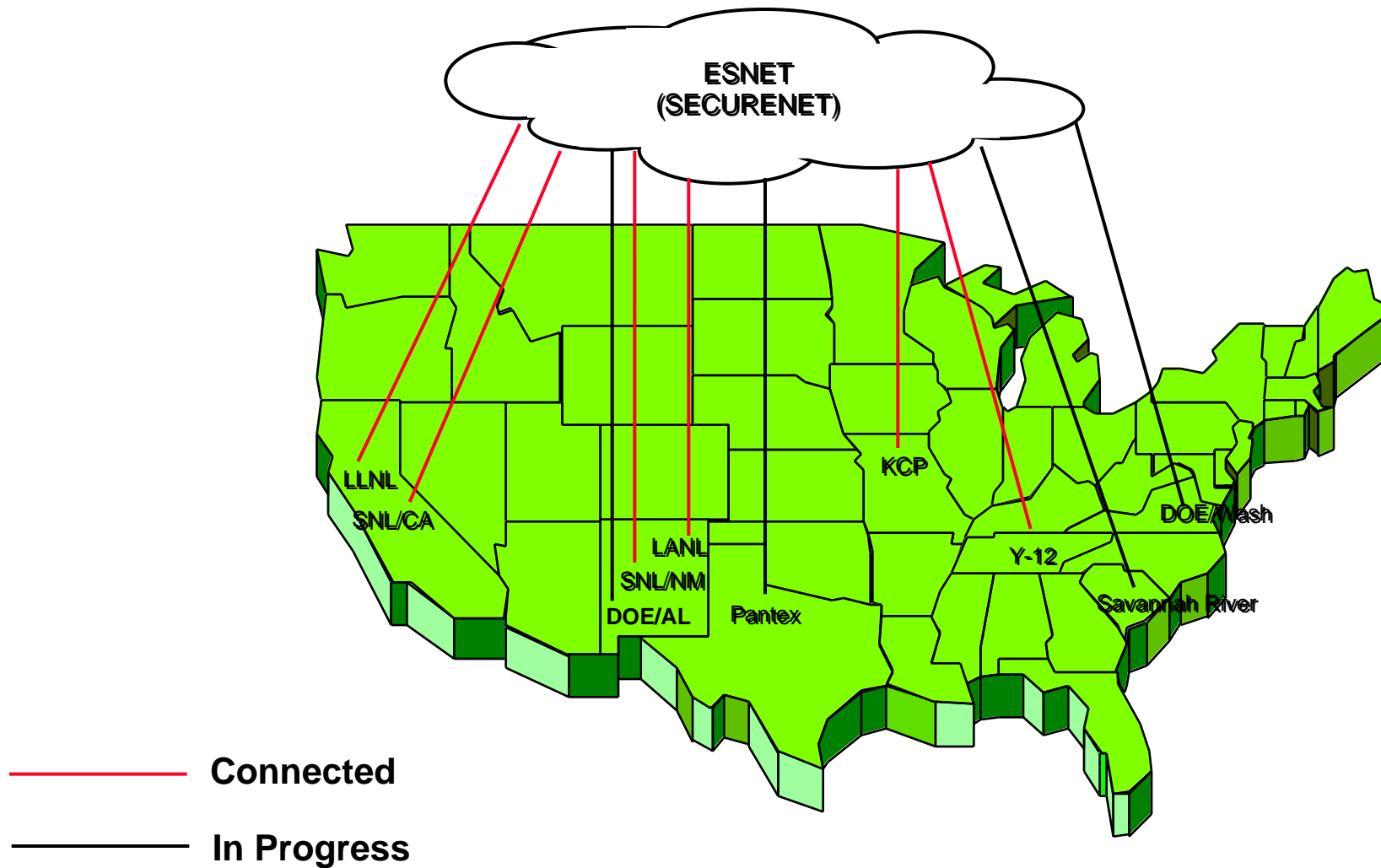
Environment + Models + Tools and Processes



In October 1995, SecureNet Linked Classified Networks at Three DP Laboratories



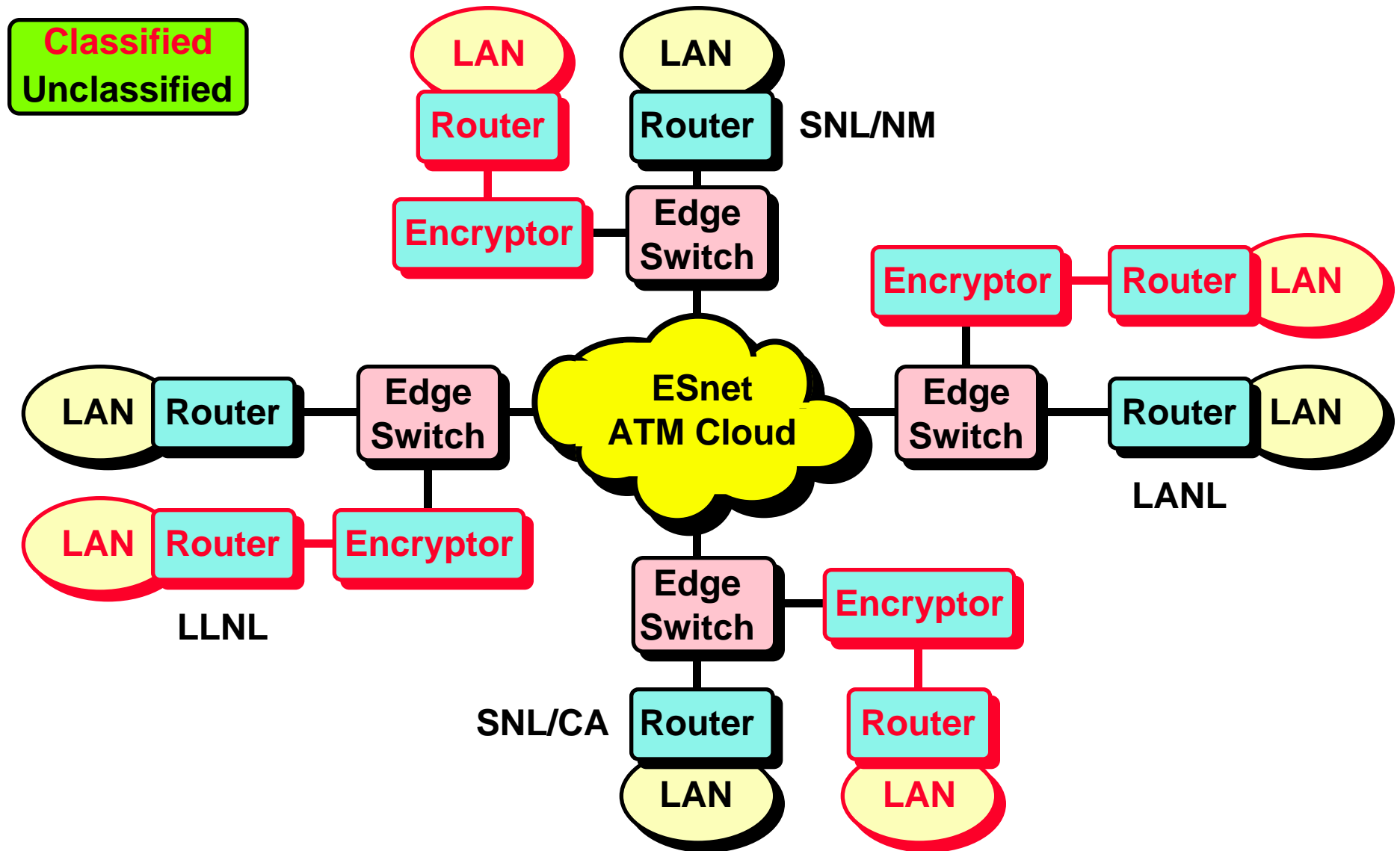
SECURENET now connects DP Laboratories and Production Plants



The Network will Offer Three Accesses

- **“Open Access” (pure ESNet) for completely unrestricted access**
- **“Restricted Access” for connecting Restricted Access Unclassified Networks**
- **“Secure Access” for connecting classified networks**

End-to-End Encryption Eliminates Dedicated Links



Encryption Performance is Key Element

- | **October 1995 through today - Motorola NES (1.5 Mb/s)**
- | **Eight FastLane encryptors (155 Mb/s) delivered February 1997**
- | **Several OC-12 (622 Mb/s) interfaces ordered**
- | **Both NES and FastLane encryption service offered**

Initial Testing of FastLane Underway

- | **FastLanes shipped to LLNL, LANL, SNL and Y-12**
- | **FastLanes configured and tested on SNL/LLNL testbed**
 - back-to-back testing at OC-3 rates with 8 PVCs
 - LLNL to SNL/CA testing in progress
- | **All-sites workshop scheduled for May 1 and 2**
- | **Final network design for FastLane integration in process**

Significant Advancements in ATM Encryption are Anticipated

- | Requirements for high-speed ATM encryption registered with NSA**
- | June 1996 meeting with NSA began intense collaboration between SNL and NSA**
- | General design architecture established for ATM encryption scaleable to OC-192 (10 Gbps)**
- | Final component design requirements established**
- | Design responsibilities divided between SNL and NSA**
- | Produce a working proof-of-principle prototype (OC-48) (end of FY97)**

“Sensitive” Unclassified Information - A Large Portion of Intersite Traffic

- | Goal - provide DES encryption service between sites**
- | Site must protect data on “Restricted Network”**
- | Analysis of firewalls separating Open and Restricted Networks at each site**

SecureDomain Encryptor

- **NIST approved DES Encryption Algorithm**
- **Simultaneously encrypts IP, IPX and Appletalk**
- **Supports up to 256 networks or subnets**
- **Selectively encrypt/decrypt based upon IP address**
- **Supports AUI, 10BASE2 and 10BASET interfaces**
- **3.5 Mb/s throughput - next version capable of 6-8 Mb/s**

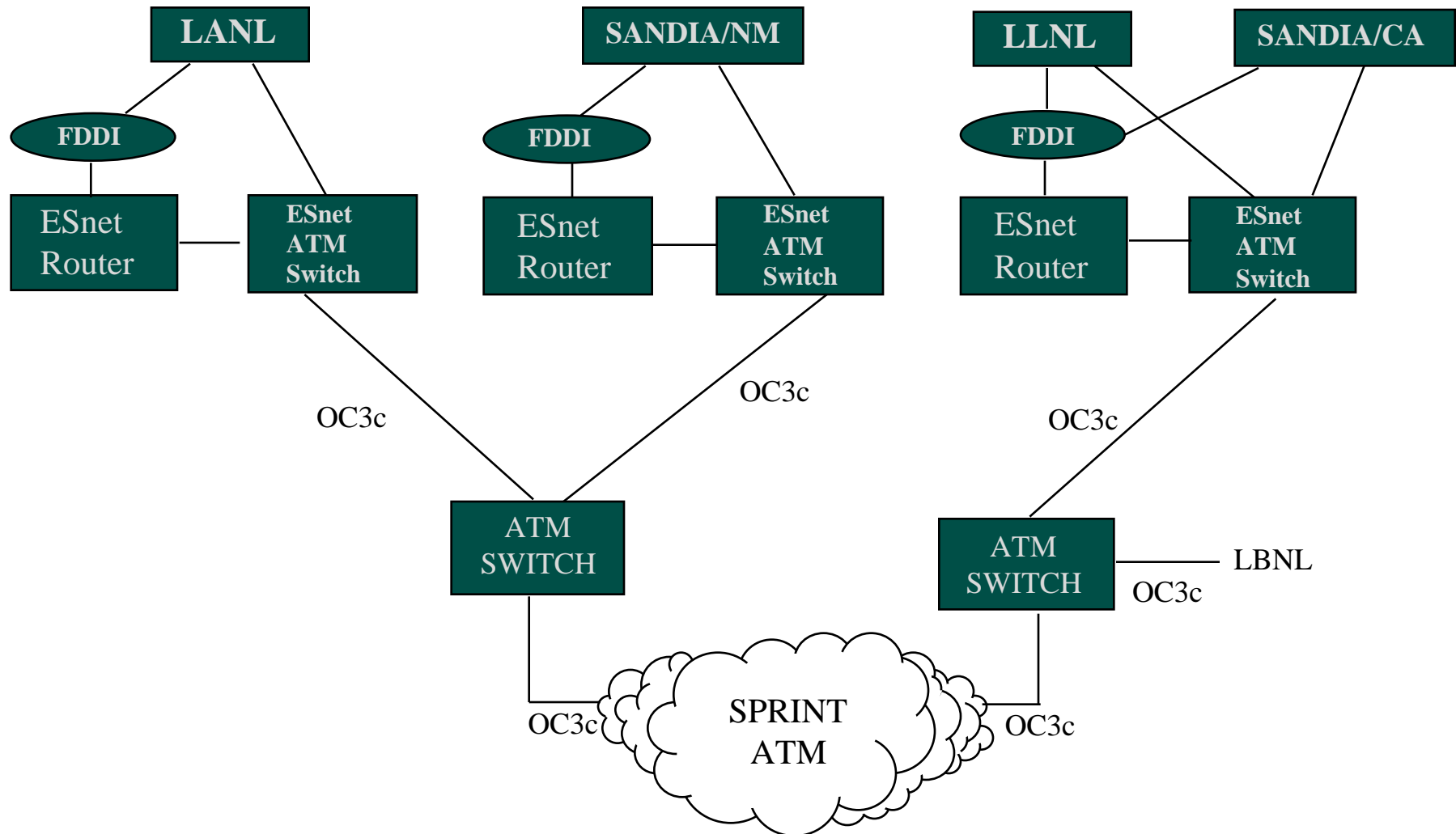
SecureDomain Testing Underway

- | **Testbed established between SNL/CA and ASKCD over ESNet**
- | **Throughputs of 424 Kb/s achieved for ftp file transfers**
- | **No difference in throughput for encrypted and unencrypted files**
- | **Throughputs constrained by bandwidth**

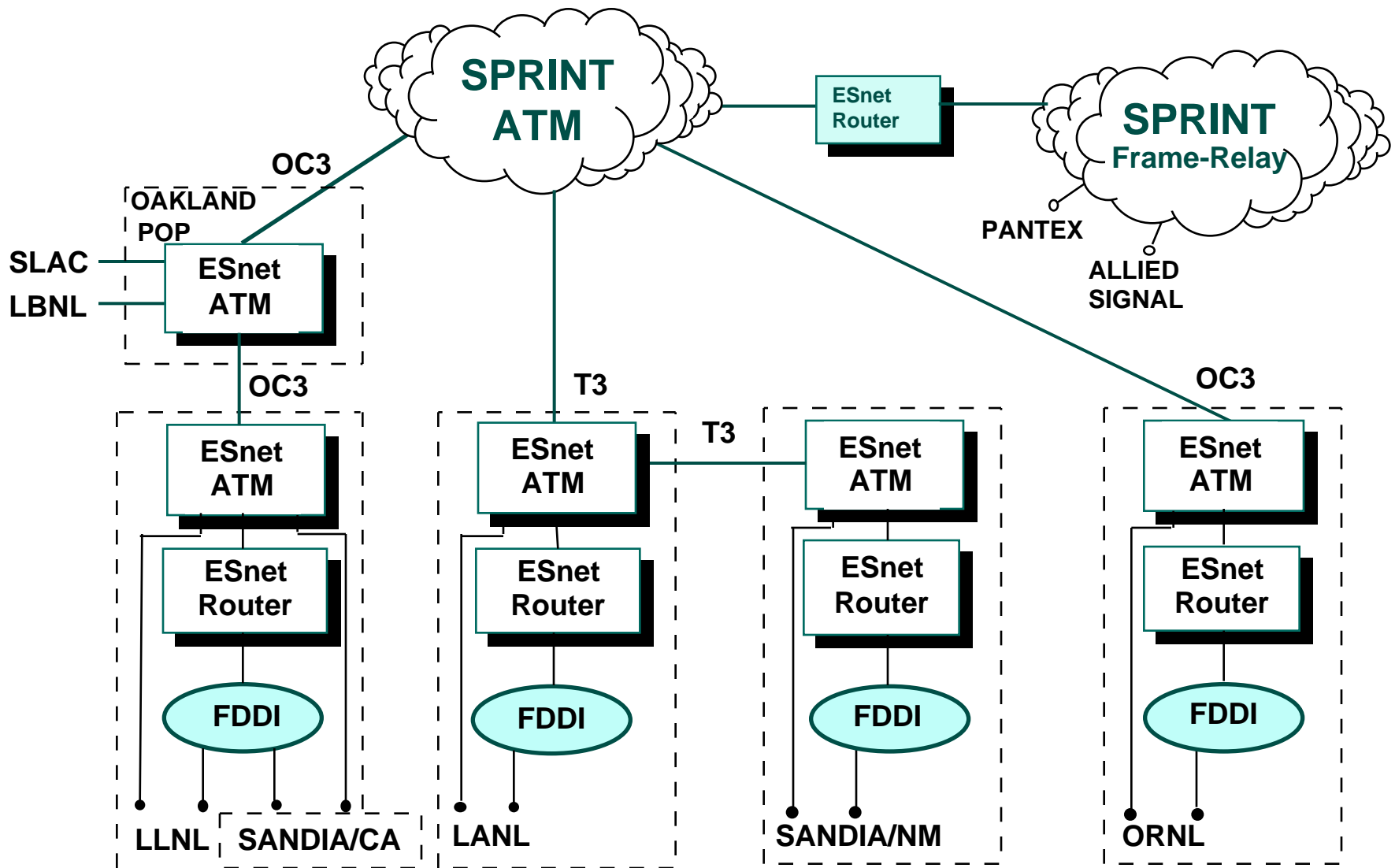
Intersite Network Speeds will Reach 155 Mbps.

- **A shared strategy makes OC-3 intersite bandwidth possible**
 - **SNL/NM and LANL will share one port**
 - **SNL/CA and LLNL will share one port**
 - **DP and ER will share access**
- **Cost for shared OC-3 approach equal to dedicated DS-3 costs**
- **Shared approach should benefit bursty experimental traffic during FY97**

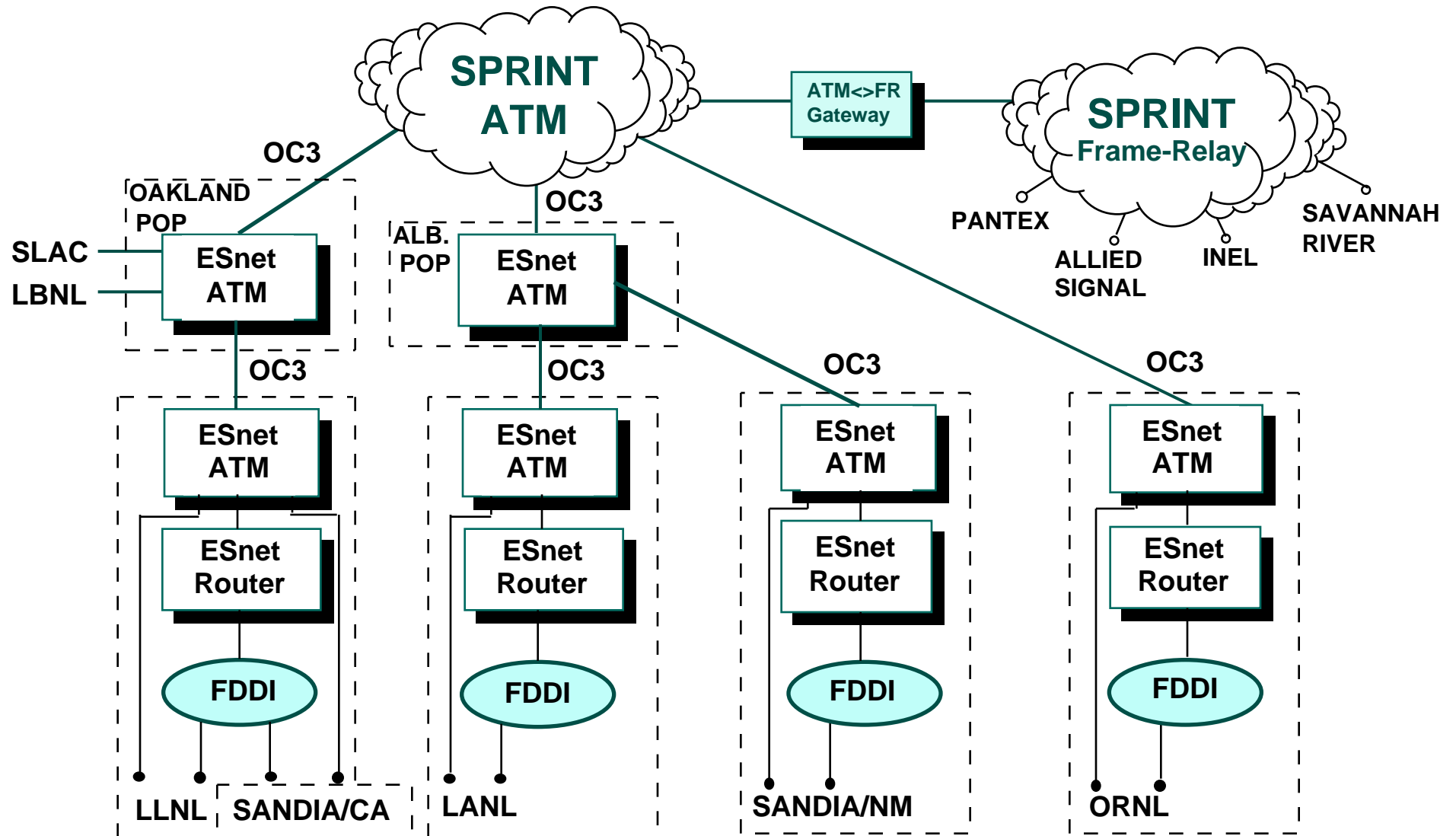
SecureNet: SHARED OC3c ACCESS



SecureNet - Current



SecureNet - 1997

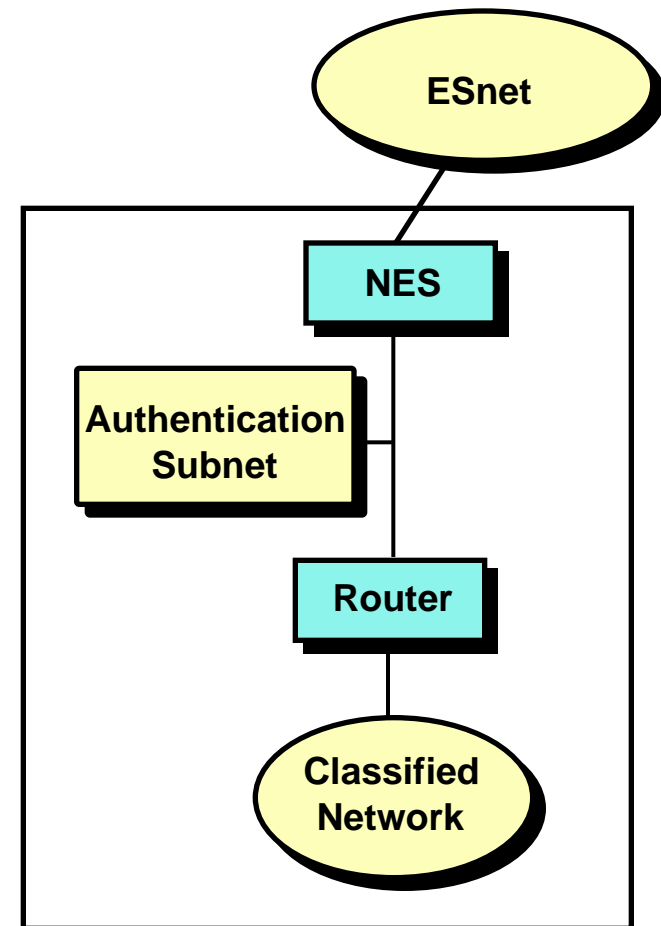


Common Authorization Scheme has been Established

- | A common “guest account” form is used**
- | Classified fax machines and STU-3 telephones have been installed**
- | Password control organizations are teaming**
- | A web site is under development**

Phase I authentication observes local policies

- | **Authentication subnet at each laboratory**
- | **Users telnet to authentication subnet and follow local authentication policies (e.g., Kerberos)**
- | **Massive replication of Kerberos client software avoided**



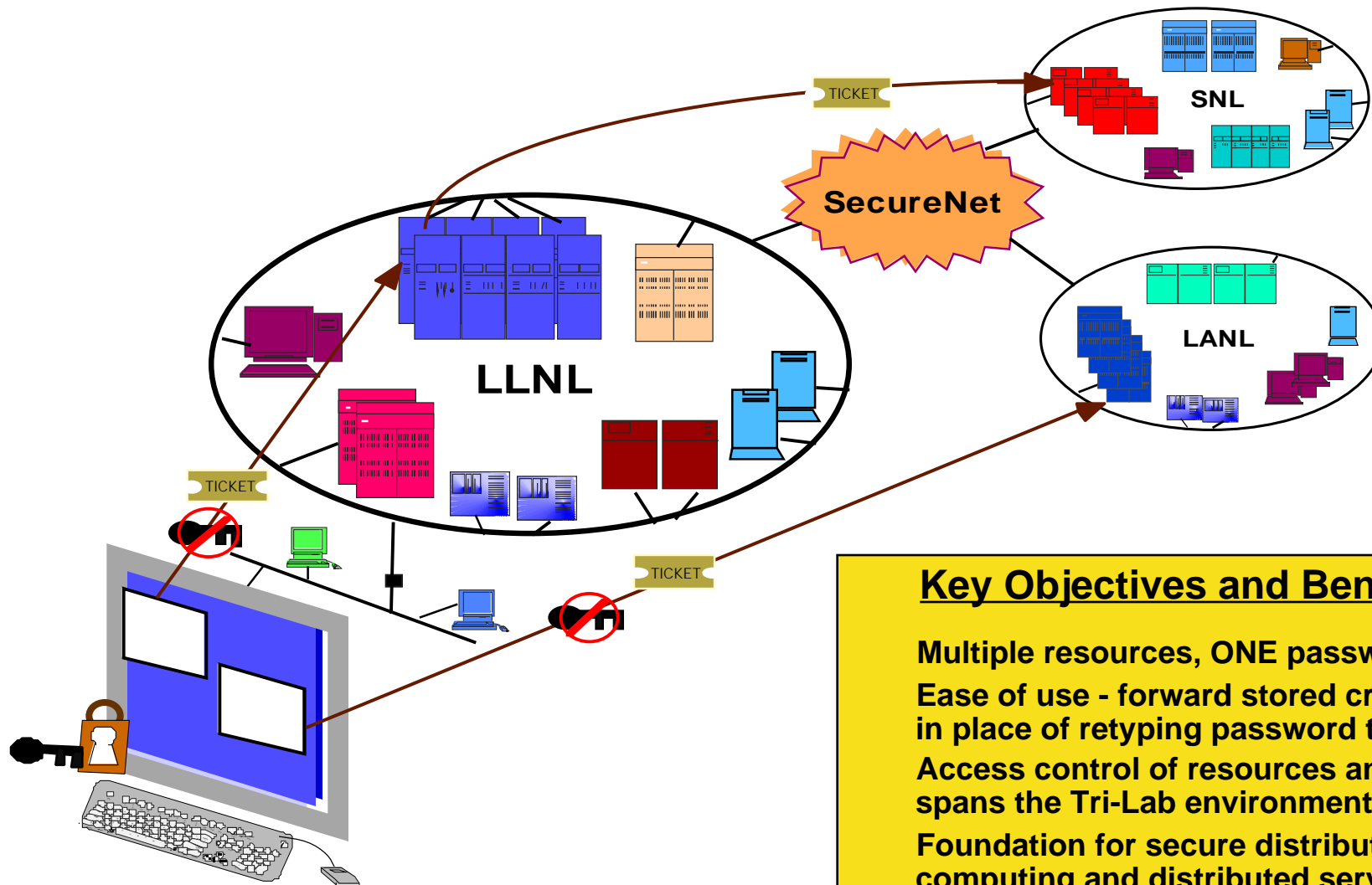
SecureNet Only Comes to the Front Door

- | **General philosophy - each site protects itself**
- | **Limited number of machines (Crays and servers) currently available**
- | **Maintaining need-to-know is a major issue**

Phase II authentication uses DCE/Kerberos

- | DCE security servers on classified and unclassified networks**
- | DCE clients on local machines**
- | Cross-realm authentication common to all sites**

Secure single sign-on from desktop to platforms using DCE

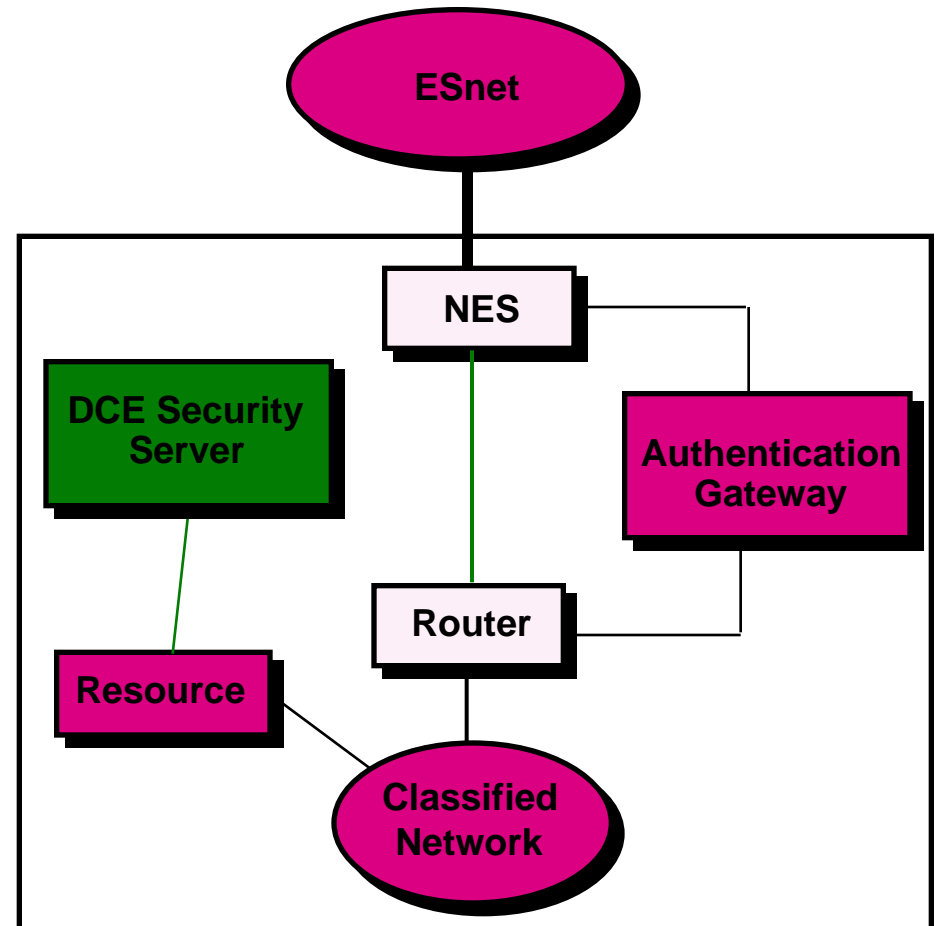


Key Objectives and Benefits

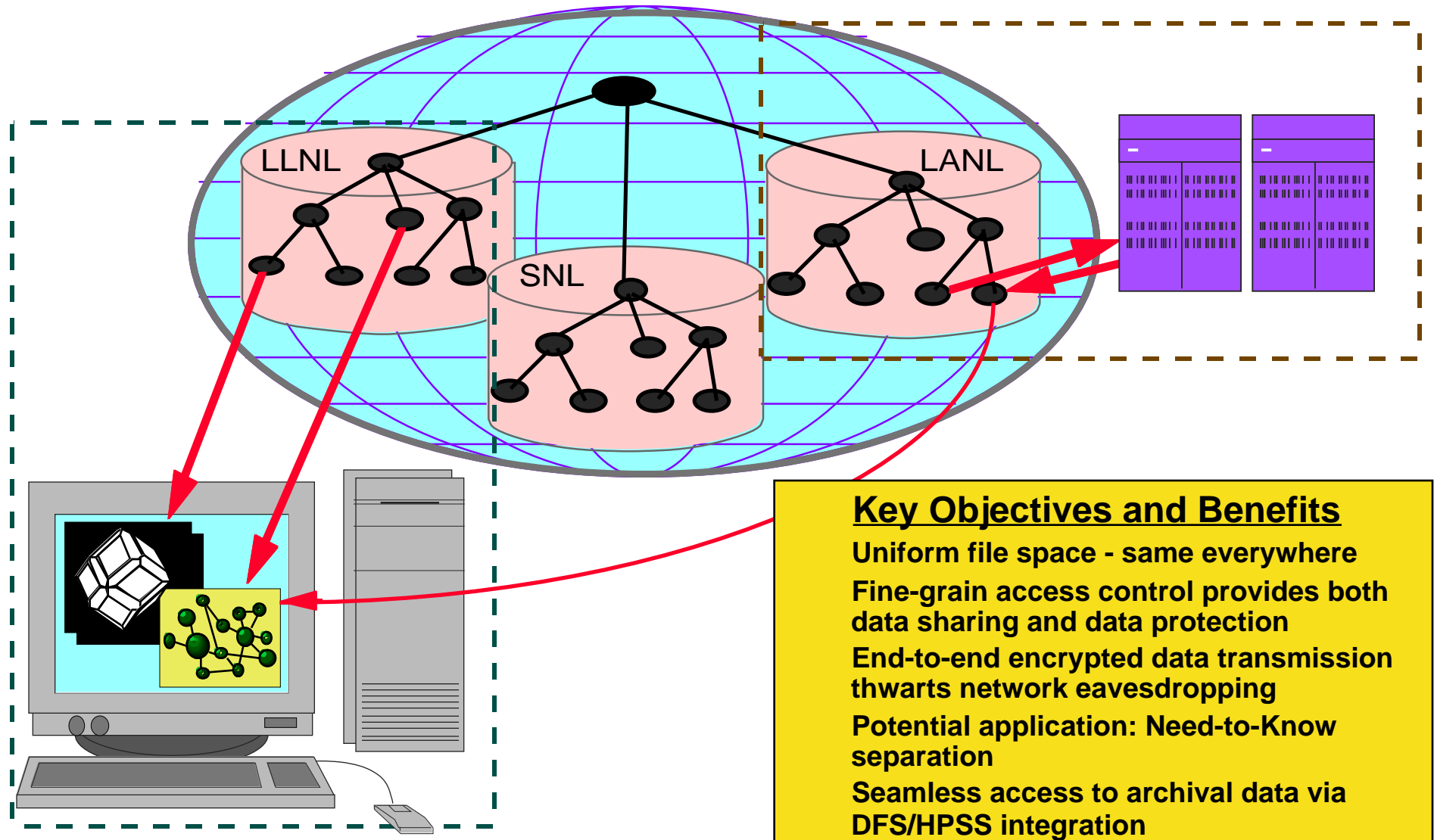
- Multiple resources, ONE password
- Ease of use - forward stored credentials in place of retyping password to login
- Access control of resources and data spans the Tri-Lab environment
- Foundation for secure distributed computing and distributed services
- Tri-Lab trust with site autonomy

Phase II Authentication

- | Phase 1 access supported for legacy systems
- | Users may now access resource directly using SSH or Kerberos utilities and resource will authenticate user using DCE security server



Tri-Lab Global file system built on DCE/DFS



Integration of DCE with Other Technologies

- **Public key (Entrust)**
- **DCE Web (DASCOM, Gradient, Intellisoft)**
- **Distributed objects (CORBA)**
- **HPSS/DFS integration**

Today, Our Focus is on Adding Services

- With the exception of encryption, bandwidth is basically related to dollars
- Achieving additional service functionality requires technology

SNL TeraFlop Computer, March 31, 1997



Conclusion: A Separate TeraFlops LAN

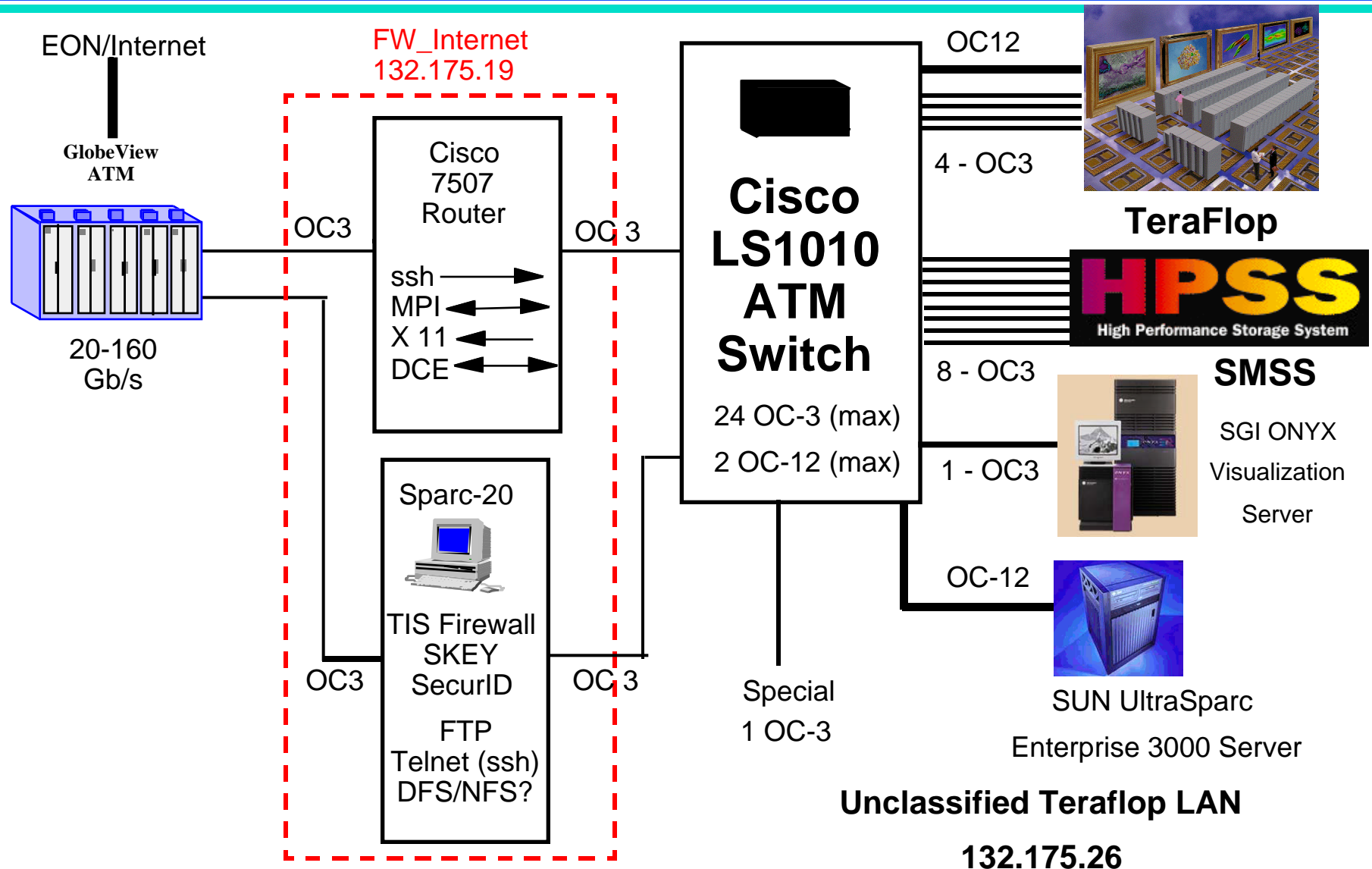
Advantages

- Protection requirements can be unique to the TeraFlops community
- Modifications to LAN protection only need approval of TeraFlops users
- Diodes between this LAN and others can be determined case-by-case

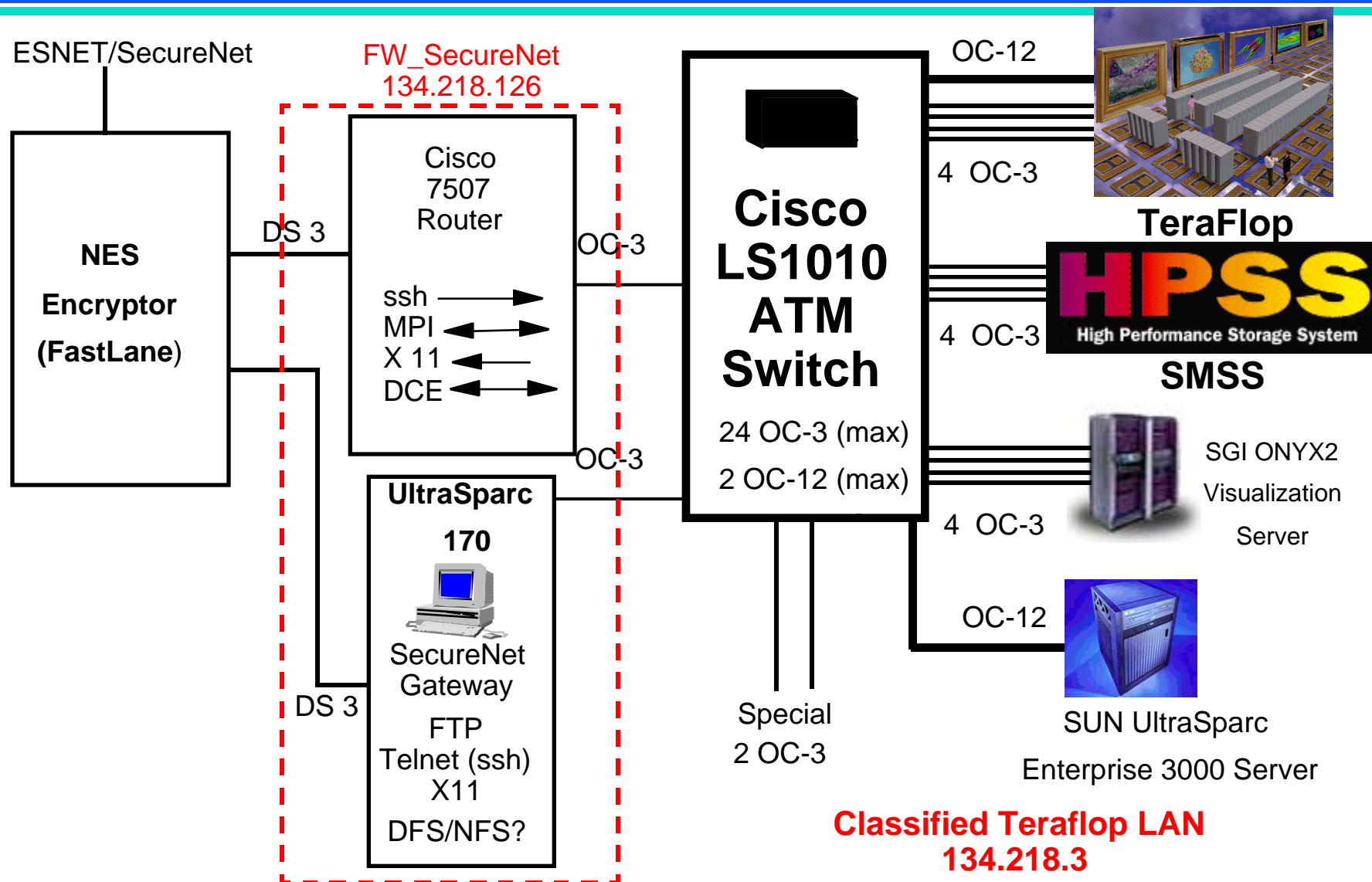
Disadvantages

- All TeraFlops users have indirect connectivity and attendant performance
- All TeraFlops users must rely on user space on the TeraFlops LAN
- LAN requires its own set of protection resources (hardware and software)

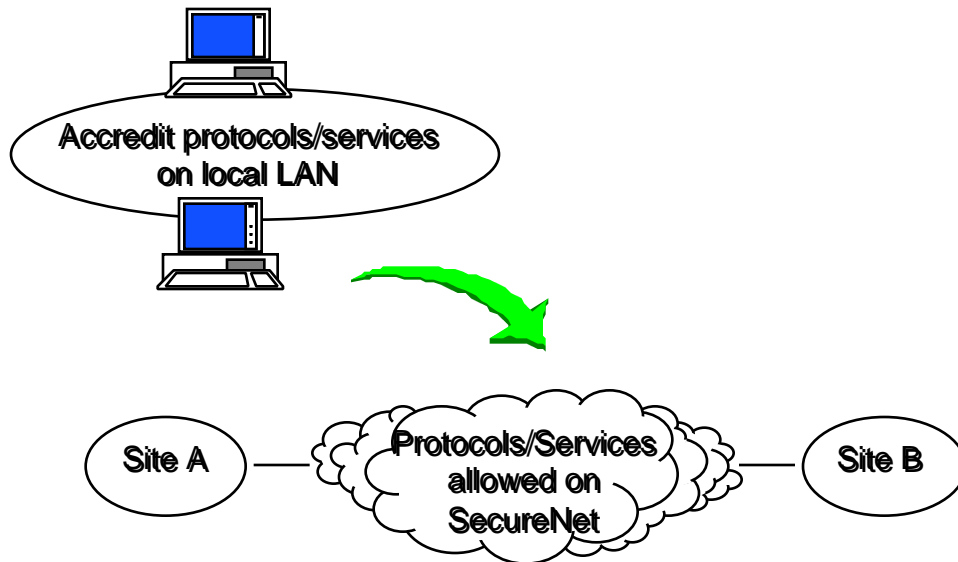
Unclassified TeraFlop LAN



Classified TeraFlop LAN



New Network Services and Protocols



Objective

Introduce needed protocols/services onto SecureNet.

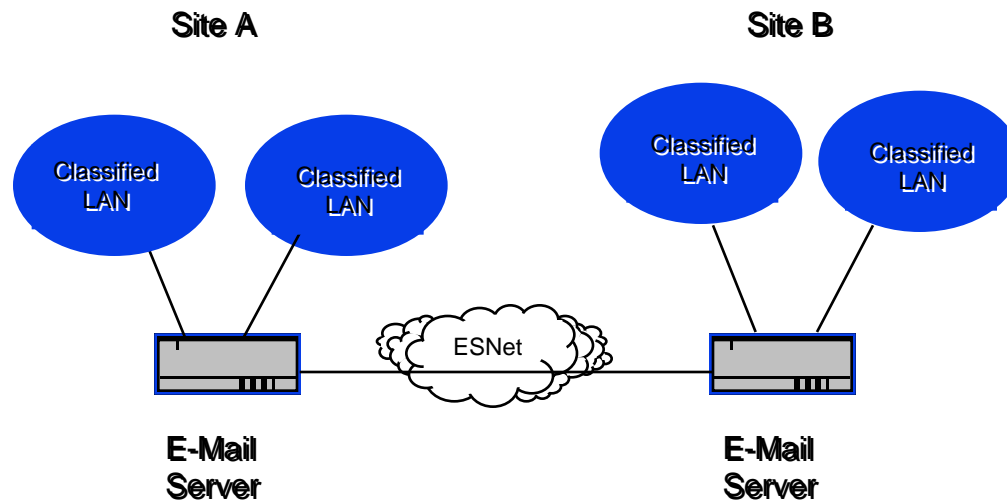
Approach

- Establish a consistent method for achieving accreditation of services/protocols
- Utilize common, controlled software across all sites
- LAN accreditation leads to WAN accreditation

Schedule, Funding, and Milestones

- Q1 FY96 - FTP and Telnet
- Q4 FY96/Q1 FY97 - X-window
- Q1 FY97 - SSH
- Q4 FY96/Q1 FY97 - Domain Name Service
- Q2 FY97 - Classified E-mail

Classified E-mail - Vital Element of Inter-Laboratory Support Structure for ASCI



Objective

Provide a classified e-mail service

- accessible to all classified LANs at each site
- integrated between sites
- maintains need-to-know separations

Approach

- Use push/pull concept to move files from sender to recipient
- Employ a server on a dedicated LAN
- Common software at all sites
- "Identical" security plans at all sites

Schedule, Funding, and Milestones

- Funding shared between ASCI and core
- Q4 FY96 - servers currently available
- Q4 FY96 - LANL created DOE-approved basic security plan
- Q2 FY97 - intralaboratory service established
- Q3 FY97 - interlaboratory service established

New Technologies for Enhanced Security and Need-to-Know Separation

- **A major emphasis during FY97**
- **Close teaming with DCE group**
- **Collaboration with vendors on beta tests**
- **Identified technologies include**
 - **SSH**
 - **virtual LANs**
 - **HTTP**
 - **Entrust**
- **The existence of SecureNet is impacting local secure networks**

State-of-the-Art Network Management is Critical

- | Some sites (LLNL, SNL, and LANL) have SNMP-based network management systems**
- | Remaining sites plan to install SNMP network management systems**
- | Sites will have capability of ping, ftp, and telnet to limited sources at other sites**
- | Working relationships are forming between operations personnel at all sites**
- | A “user reflector” will notify users of operational problems**